… Created by Mike Bloomfield

'Disaster Recovery'

September 2004

Oh My God – My computer's dead!

Plamen Pazov
Xyber Data Recovery
Xyber Computer Service Centre Pty Ltd
28 Chandos St – St Leonards – NSW 2065
Tel (02) 9906 7976, Fax (02) 9906 3620
http://www.xyber.com.au/Contact.html

DON'T PANIC!

That's when we all make mistakes.
Unfortunately, in this situation, a mistake can be very costly!
Generally, the more important your data, the slower you should proceed.
Do not try every piece of repair software that you come across.
Every attempt to "repair" the directory will overwrite some part of it and will almost always make things worse. Any attempts should only be done on a Sector Clone.

Repair or recovery?

In many instances, once the underlying problem has been resolved, all your data will come alive.
Be wary of shoddy operators that may attempt to sell you a new computer because there's a virus on yours that makes it play Doggo.
Make sure that whoever is dealing with the problem has a clear idea what the actual issue is.
Make doubly sure the hardware's working BEFORE attempting ANY software repair or reinstallation.

Hardware / System / Applications / Documents

Any computer consists of a number of interrelated parts.
As a general rule, a part will not work unless the underlying infrastructure works.
The minimum configuration will include:

A set of hardware parts that (hopefully) work together

Processor and Memory on a motherboard providing interconnections and input/output interfaces;
Storage devices – Hard disk drive, CD drive, Floppy drive;
Input/output devices – Keyboard, Mouse, Display.

An Operating System

Windows
Mac OS
Unix / Linux
This is the set of programs that together provide a all the standard services that application programs may need – Display something, print something, save something, etc.
It includes the device drivers required to talk to specific pieces of hardware.

Application programs

These are the pieces of software a computer user will need to get some work done (eg. Word, Excel, PowerPoint, etc.) The work itself is the document.

Documents

This is your hard work – all the sleepless nights!!!
If a document fails, check whether other documents of the same application work fine. If yes, then try copying all the contents of a document and pasting them into a brand new document. This may get rid of specific problems such as crashing when printing or spell-checking, etc.

Other stuff

Check your ancillary add-ons (such as fonts). A damaged font can create havoc in all the documents containing it, yet each document in itself is perfectly OK.
An external style, which is being used within a document can be another source of problems (and a way of distributing viruses).
Incompatible or wrong device drivers are yet another major source of headaches.

Storage devices

There are two main categories:

- Block devices (random access) such as Disk drives and
- Sequential devices (streaming) such as Tape drives.

Block Devices: fixed size Sectors

All storage devices (disk drives, floppy drives, even flash cards) work in a structurally simple way: They all store information in fixed size chunks called Sectors or Blocks.
Each sector is of the same size (usually 512 Bytes/sector except CDs where it's 2048 Bytes/sector.)
Each sector is accessed by its sequential number, starting from sector 0 and up to however many sectors are available on that particular device. (So, for example, a 20 Gigabyte disk drive will contain about 40 million sectors.)

Files & Directory

Files

A file is a named logical entity of information.
Information can be added to it subsequently and it is accessed in a random fashion.
It is maintained as a logical unit by (and Only by) the operating system.
Any manipulation of the information contained inside a file is done not directly but by the application program giving instructions to the operating system.
As more information is added to a file, the operating system allocates more disk space to it in fixed size lumps called clusters.

Directory

In order to be able to manage all the files that are written to a disk, the operating system has to keep track of which clusters are allocated to which file. This information is kept right at the beginning of the disk in an area called the Directory.
Each kind of operating system has its own type of directory structure (HFS and HFS+ for Mac OS, FAT16, FAT32 or NTFS for Windows, UFS, ISO9660, etc.) but they all basically have the same function – keeping track of which files are on this disk and which sectors are allocated to which file.
In addition to a file's name, information such as when was it created, last modified, who can read it, write to it, etc. is also kept.
Note that:

- No one but the operating system is permitted to directly access a file's contents, nor the disk's directory.
- The operating system relies on the contents of the disk's directory to access and manage the files.
- A damaged or erased directory is similar to what would happen if all the pages of all the books in a library were torn off and piled in the centre: All the information is still there but working out which page belongs to which book and in what sequence could be a challenge.

What does a format do?

Instructing the operating system to format a disk drive means telling it to write a clean, new directory to it.
Great if you want to start from scratch but not good if there is still valuable information on that disk.

What happens when you erase a file?

When you erase a specific file or a whole bunch of them (as in erasing a whole folder containing files), you are in fact instructing the operating system that the data contained in those files is no longer required and therefore that it can use the allocated disk space for other needs.
In effect you are declaring the allocated disk space available.
Note that even though the file entry has been removed from the directory, the actual information won't be overwritten until that space is required for use by another file. Therefore, if you erase a file by mistake, stop using the computer immediately and take it to experts such as Xyber.

Recovery sequence

Hardware -> Directory -> Files
You can't build a house without first laying foundations!
Put simply, attempting to repair a directory that's sitting on bad blocks is guaranteed to make things worse.
It is imperative to make sure one layer is working before even testing functions of the layer above it.

Don't work on the original -> Always Make a Clone

If you're only allowed one byte at the cherry, get a whole basket of cherries!
Be VERY weary of people (or utilities) that claim that they can "repair" your drive – the directory of a damaged drive is even more fragile than a good one's because there are no active protective processes filtering every access to that part of the disk.
By making a sector clone of your disk drive onto another known good drive, we avoid the chance of irreparable damage – we can always go back to the source and make another clone.
As an extra incentive, we are working with a known good piece of hardware - so we are not taking chances with possible intermittent bad blocks or other potential hardware problems.
The original should be left alone until all the data is safely out of harm's way.
Then – and only then – a full low level format with complimentary pattern tests should be run on the original disk drive, and if all is well, the device reinitialised and a new volume and directory created.
Only after all of the above, can we safely move the recovered data back onto the original disk drive.
If at all possible, the operating system and applications should be reinstalled.

Other types of recovery

If the directory information has been completely overwritten and there is no file information left, then we can search for markers of the beginning of a particular type of file (.doc, .jpg, .avi, etc.)
These are called File Header Signature searches. They can be effective and work well but can collect extraneous data that simply looked like the beginning of a particular kind of file. Also, as there is no directory information, these searches yield no file names or directory information. The user will have to go through these files, open and resave the useful ones under a meaningful name. This can be a laborious task but is a lot better than no data at all.
There are other options such as text or binary searches – in extreme cases only.

What if you really want to erase a file!

There are a whole lot of utilities out there on Internet Land that allow you to completely erase a file from a hard disk drive. Usually, these utilities first overwrite all the clusters allocated to that file with a number of patterns and only then do they erase the file in a normal way.

How to avoid the problems:

Prevention is the best cure!

Archive stuff you don't need – you'll need it someday!

Transferring older and less used files to archival media such as CD-ROM is a very good way to force yourself to clean up, free up disk space and organise your workspace.

Backup

Automatic backup – if it's automatic, it will happen. Otherwise, when you get busy, the backup falls by the wayside and that's when things really get nasty.
Directory backup – the backup you do when you don't have a backup…
File synchronisation – poor man's backup.
Internet backup – for the really important stuff. (For small files only but at least it's safe.)

Get your computer checked regularly

This can find problems before they turn into disasters.

Maintenance

Make sure there is enough workspace available –> Archive.
Virus checks
Directory checks
File checks

What NOT to do!

Again, first and foremost:
DON'T PANIC!
Don't try on every piece of "repair" utility that your well-meaning friends throw your way.
Don't do any changes to the original disk drive until you are happy with whatever data has been recovered onto a separate good disk.
Don't only recover the files that are currently important – Get Everything – There is always one more important file that you'll remember once the original drive has been reformatted.

By

Plamen Pazov
Xyber Data Recovery
Xyber Computer Service Centre Pty Ltd
28 Chandos St – St Leonards – NSW 2065
Tel (02) 9906 7976, Fax (02) 9906 3620
http://www.xyber.com.au/Contact.html

Plamen is a true genius in our field and a leading expert on data recovery, photo recovery and all things MacIntosh. I am refreshed as he enlightens misunderstood areas of our industry with absolute clarity and precision – and authority.
Please feel free to contact Plamen and his brilliant team at Xyber for unparalleled advice and service. There are few businesses I have found in any sphere of activity that share the integrity, honesty, ethical standards and enthusiasm that this team zealously uphold.
Little wonder our leading Television and Radio networks, I.T. professionals and the elite of Graphics Design champion his outstanding service and unique craft year in, year out!

Kind Regards,

Mike Bloomfield